The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/10/2017

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Google Chrome prior to 57.0.2987.98

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote code execution. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- Memory corruption in V8 (CVE-2017-5030)
- Use after free in ANGLE (CVE-2017-5031)
- Out of bounds write in PDFium (CVE-2017-5032)
- Integer overflow in libxslt (CVE-2017-5029)
- Use after free in PDFium (CVE-2017-5034)
- Incorrect security UI in Omnibox (CVE-2017-5035)

- Use after free in PDFium (CVE-2017-5036)
- Multiple out of bounds writes in ChunkDemuxer (CVE-2017-5037)
- Use after free in PDFium (CVE-2017-5039)
- Information disclosure in V8 (CVE-2017-5040)
- Address spoofing in Omnibox (CVE-2017-5041)
- Bypass of Content Security Policy in Blink (CVE-2017-5033)
- Incorrect handling of cookies in Cast (CVE-2017-5042)
- Use after free in GuestView (CVE-2017-5038)
- Use after free in GuestView (CVE-2017-5043)
- Heap overflow in Skia (CVE-2017-5044)
- Information disclosure in XSS Auditor (vampire) (CVE-2017-5045)
- Information disclosure in Blink (CVE-2017-5046)

Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Google:
https://chromereleases.googleblog.com/2017/03/stable-channel-update-for-desktop.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5029
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5030
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5031
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5032
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5033
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5034
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5035
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5036
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5037
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5038
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5039
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5040
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5041
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5042
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5043

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5044
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5045
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5046